Annex: A Comparison of the major digital trade provisions under TCA, CEPA, CPTPP, Australia-Singapore DEA and USMCA

	TCA	CEPA	CPTPP	Australia-Singapore- DEA	USMCA
Non-discriminatory treatment of digital products	**No**	**No**	**Yes:** Art. 14.4: Non-discriminatory treatment of "digital products" *Exception: rights and obligations under the TRIPS Agreement, subsidies, grants, and broadcasting.	**Yes**: Art. 6: Non-discriminatory treatment of "digital products" * A copy from CPTPP *Exception: rights and obligations under the TRIPS Agreement, subsidies, grants, and broadcasting.	**Yes:** Art 19.4: Non-discriminatory treatment of "a digital product" *Exception: a subsidy or grant provided by a party
Free data flow	**Yes**: Article DIGIT.6. Cross-border data flows (6.1) *Free data flow based on right to regulate (DIGIT 3) and exceptions (DIGIT 4). *The language is an endeavour clause ("*The parties are committed to ensuring cross=border data flows……*") *Implementation of the provision will be reviewed within three years (6.2) *Primacy of protection of personal data and privacy over free data flow (DIGIT 7)	**Yes**: Article 8.84: Cross-border transfer of information by electronic means *The stronger language of prohibition than CPTPP ("*A Party shall not prohibit or restrict the cross-border transfer of …*") *Exceptions: The strong legitimacy requirement to pursue public policy objective (Art. 14.11.3(a) and (b)), a copy from CPTPP	**Yes**: Article 14.11: Cross-border transfer of information by electronic means *Recognition that each Party may have regulatory requirements for data transfer *The weaker language of prohibition than CEPA ("*Each Party shall allow the cross-border transfer of….*") *Specific reference to 'personal information' *Exceptions: The strong legitimacy requirement to pursue public policy objective (Art. 14.11.3(a) and (b))	**Yes**: Cross-border transfer of information by electronic means *Recognition that each Party may have regulatory requirements for data transfer, a copy from CPTPP *The strong language of prohibition (*"Neither Party shall prohibit or restrict…*") *Specific reference to 'personal information' * Exceptions: The strong legitimacy requirement to pursue public policy objective (Art 23.3 (a) and (b)), a copy from CPTPP	**Yes**: Art 19.11: Cross-border transfer of information by electronic means *The strong language of prohibition (*"No Party shall prohibit…*") *Specific reference to 'personal information' * Exceptions: The strong legitimacy requirement to pursue public policy objective (Art 19.11 (a) and (b)), slightly stronger language than CPTPP

Data protection and privacy,	**Yes** : Article DIGIT7: Protection of personal data and privacy *Reference to data privacy as a fundamental right (7.1) *Protection of personal data and privacy as a condition of cross-border data transfers (7.2) *Each Party is required to inform any changes of data protection measures (7.3) *The EU separately accorded an adequacy decision to the UK (June 2021) with a four years sunset clause.	**Yes**: Art. 8.80: Personal information protection *A full copy from CPTPP *Plus, the UK and Japan accorded adequacy decision on data protection to each other. .	**Yes**: Art, 14.8: Personal information protection *In developing a legal framework, ”*Party should take into account principles and guidelines of relevant international bodies*”. (Art.14.8.2) *To promote compatibility between different regimes, autonomous recognition, mutual arrangement or broader international frameworks are mentioned. *No specific reference to APEC Privacy Framework (Art 14.8.2 and 14.8.5)	**Yes**: Art. 17: Personal Information Protection *Basically CPTPP approach but go much further towards business driven system. *In developing a legal framework, ”*Party should take into account principles and guidelines of relevant international bodies*”. A specific reference to APEC Privacy Framework and the OECD recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transsborder Flows of Personal Data (Art. 17.2). *Recognition of CBPR System (The APEC Cross-Border Privacy Rules) as a valid system and promotion of the System (Art.17.8 and 17.9)	**Yes:** Art. 19.8: Personal information protection *In developing a legal framework, ”*Party should take into account principles and guidelines of relevant international bodies*”. A specific reference to APEC Privacy Framework and the OECD recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data. (Art. 19.8.2). *APEC Cross-Border Privacy Rules system is recognised as a form to promote compatibility between the different regimes (Art.19.8.6).
Ban on Data localisation	**Yes**: Article DIGIT.6: Cross-border data flows (6.1) *Ban on data localisation requirements based on right to regulate (DIGIT 3) and exceptions (DIGIT 4). *The review clause (6.2) *Primacy of protection of personal data and privacy over free data flow (DIGIT 7)	**Yes**: Article 8.85: Location of Computing facilities *Exceptions: Strong legitimacy requirements (Art. 8.85.3) but without necessity requirement.	**Yes**: Art. 14.13: Location of Computing facilities *Recognition that each Party may have its own regulatory requirements (Art. 14.13.1) *Exceptions: Strong legitimacy requirements to pursue public policy objective (14.13.3)	**Yes**: Art. 24: Location of computing facilities *Recognition that each Party may have its own regulatory requirements (Art. 24.1) *Exceptions: Strong legitimacy requirements to pursue public policy objective (24.3)	**Yes**: Art. 19.12 Location of computing facilities *The strong language of prohibition (*“No Party shall require…*”) *No exception clause

			*The conditions are stricter than CEPA	*A copy from CPTPP except for a clause on ban of data localisation for financial services (Art. 25), which does not exist in CPTPP.	
Ban on disclosure of Source code	**Yes**: DIGIT. 12: Transfer of or access to source code *Ban on transfer of or access to source code of software (the scope is narrower than CEPA) *Reference to Exception (DIGIT. 4) for a certification procedure *Safeguarding exception clauses covering competition law, public safety, IRPs and Government Procurement Agreement (DIGIT. 12.3)	**Yes**: Article 8.73: Source Code *Ban on mandatory requirement of the transfer of, or access to source code of software and related algorithms *The scope is wider than TCA and CPTPP. *Safeguarding exceptions (Art. 8.72.2, 3 and 4), similar to TCA	**Yes**: Art. 14.17: Source code *Ban on mandatory disclosure of source code (the scope is narrower than CEPA, Australia-Singapore DEA and USMCA). *Narrower safeguarding exceptions than CEPA.	**Yes**: Art. 28: Source code *Ban on mandatory requirement of the transfer of, or access to source code of software and related algorithms *No exception clause for the clause but the WTO type General exceptions (Art.3) is applied	**Yes**: Article 19.16: Source code *Ban on mandatory requirement of the transfer of, or access to source code of software and related algorithms *Exceptions: Not so specific as TCA and CEPA. *Reference that trade secret should not be negatively affected (Art. 19.16.2, footnote 2)

Note 1: "Yes" means there are provisions for the issue. As the gradation of the blue in the column of 'Yes' becomes lighter, reflection of public policy objective (e.g. inclusion of provisions to retain government interventions to safeguard safety, security and privacy) becomes weaker: Yes (Strong degree of safeguard provisions)→ Yes (less strong safeguard provisions in detail), → Yes (limited degree of safeguard provisions) → Yes (no/very limited degree of safeguard provisions)

Note 2: No means no provision for the issue.